



Premier Services Evaluation Report

**For:
Anchiva Systems, Inc.
Anchiva-2000X
Firmware Version 2.0**

Original Publication Date:
April 18, 2007

Prepared by:

ICSA Labs Corporation
1000 Bent Creek Blvd
Mechanicsburg, PA 17050

Anchiva Systems, Inc. Anchiva-2000X version 2.0

Executive Summary

Introduction

ICSA Labs Premier Services offers customized evaluation and certification testing services for information technology products and solutions. For each product submitted for evaluation testing, ICSA Labs develops a test methodology for the customer's individual needs. The customized methodology is based on test processes from existing ICSA Labs programs as well as input from the vendor of the submitted product, industry experts, and Premier Services Alliance Partners. After the customized evaluation test methodology is finalized, ICSA Labs tests the submitted product against the methodology.

Product Overview

The product evaluation for this engagement focused on a security product developed by Anchiva for sale as an anti-spyware and anti-malware secure web gateway. Anchiva's Anchiva-2000X is intended to detect content-based threats from Internet traffic without degrading network performance.

Note, the Anchiva systems maintain a single malware database which includes both virus and spyware signatures. The terms "anti-malware" and "malware" will be used to denote both anti-virus and anti-spyware.

Scope of Assessment

Anchiva Systems, Inc. (Anchiva) contracted ICSA Labs Premier Services to evaluate the Anchiva-2000X running AnchivaOS and firmware version 2.0. The goal was to evaluate the Anchiva 2000X's maximum throughput when providing content inspection of HTTP and SMTP traffic. The following is an evaluation report which details the testing conducted and documents the findings.

ICSA Labs Premier Services evaluated the product in the areas listed below, with the emphasis in each area as specified below:

- Throughput, with anti-virus scanning enabled
 - ◆ HTTP traffic only
 - ◆ SMTP traffic only
 - ◆ Mix of HTTP and SMTP traffic
- Maximum Transaction Rate, with anti-virus scanning enabled
 - ◆ HTTP traffic only
 - ◆ SMTP traffic only

Summary of Findings

Anchiva Systems, Inc.'s Anchiva-2000X running AnchivaOS and firmware version 2.0 completed testing against a customized test methodology designed to verify its performance capabilities.

To test for malware detection, ICSA labs configured web and email clients and servers on either side of the Anchiva system and transferred virus samples while the system was under load. For all throughput and transaction tests, the Anchiva-2000X was able to successfully detect, block, and log all infected web and email traffic. The Anchiva-2000X used a database of 665,252 combined virus and spyware signatures during these tests.

ICSA Labs determined the Anchiva-2000X was able to achieve the following throughput capacities:

- HTTP Performance: over 790 Mbps
- HTTP Transaction Rate: over 10,000 HTTP transactions per second
- SMTP Performance: over 415 Mbps
- SMTP Message Rate: over 2,700 messages per second
- HTTP + SMTP Concurrent Traffic Mix: over 640 Mbps
- Packet Per Second (PPS): over 109,000 packets per second

System Components

Section Introduction

ICSA Labs Premier Services requires that vendors submit for evaluation at ICSA Labs all hardware, software, and documentation necessary to execute the requested tests. For the purposes of this document, the term System Under Test (SUT) refers to the complete system submitted by the vendor to ICSA Labs to be evaluated during evaluation testing. This includes any and all documentation, hardware, firmware, software, host operating systems, management stations, etc. used to meet the custom requirements. Servers providing common management services such as Syslog and NTP are provided by ICSA Labs and are not considered part of the SUT.

This section details the components of the SUT submitted by Anchiva for evaluation, as well as any relevant components supplied by ICSA Labs.

Hardware and Software

Anchiva supplied a single Anchiva-2000X anti-malware scanning gateway with dual power supplies and eight copper Gigabit Ethernet interfaces. The Anchiva-2000X was running AnchivaOS and firmware version 2.0.0.1001.47 with version 1.03 of its Scan Engine, version 2.0 of its Inspection Engine with Malware Definitions 1000.45, and version 1.0 of its Spylist Engine with Spylist Definitions 1000.00. The Anchiva-2000X's Malware Definitions were last updated immediately prior to testing on April 7, 2007 and contained 655,252 combined virus and spyware signatures. The Anchiva-2000X was managed primarily through a standard web browser.

Spirent WebAvalanche 2500 and WebReflector 2500 network test appliances running version 7.50 were used for the performance portion of these tests.

ICSA Labs supplied the LAN environment for testing, including two Gigabit Ethernet switches, a client PC running a standard email client and web browser, and a server hosting SMTP and HTTP services. ICSA Labs obtained an EICAR anti-virus test file from www.eicar.org for functional verification tests.

Methodology

Section Introduction

ICSA Labs Premier Services designs individual test plans for each customer to represent the features and functionality to be tested. Since products submitted for testing can often be configured many different ways, the Premier Services team frequently confronts many configuration-related decisions both before and after installing the SUT. For test purposes, ICSA Labs works with the customer to install and configure the SUT to properly exercise the relevant features and functionality of the SUT while maintaining a realistic configuration representative of how the product is intended to be used. ICSA Labs uses the provided documentation to assist with all configuration decisions. If multiple configurations were used for testing, they are detailed below with the findings.

Product Configuration

ICSA Labs Premier Services analysts deployed the Anchiva-2000X on a copper Gigabit Ethernet LAN with one interface connected to the client network and another connected to the server network. The 2000X system was deployed in a Transparent mode configuration so no IP addresses were required to be assigned to the test interfaces, although an IP address was assigned to a management interface to allow configuration of the device through the WebUI. None of the other interfaces were used during testing.

The Anchiva-2000X was configured identically for all tests. After the network interfaces were configured, analysts used the WebUI to create a policy from the "Policy" tab in the GUI to scan all HTTP and SMTP traffic, inbound and outbound. The policy was configured to inspect HTTP downloads (Gets) but not uploads (Posts). The policy was also configured to append a message to the end of all emails that had an attachment stripped by the gateway, though uninfected or clean messages were not altered. The Anchiva-2000X was not configured to scan FTP or POP3 traffic. Next the "Quarantine" option was enabled on the "Anti-virus" tab. Finally, the "Inspection Mode" was set to "Preventative".

Logging of administrative messages and malware-related events were enabled on the Anchiva-2000X, though Syslog was not used. Email alerting was disabled.

Test Description

For these tests, analysts deployed the Anchiva-2000X in the testbed as depicted in the diagram below which is designed to simulate deployment in a typical customer environment. ICSA Labs measured the performance of the Anchiva-2000X firmware by using Spirent's WebAvalanche and WebReflector network test appliances to inject and monitor network traffic. The Spirent appliances were managed using Spirent's Avalanche Commander version 7.50.

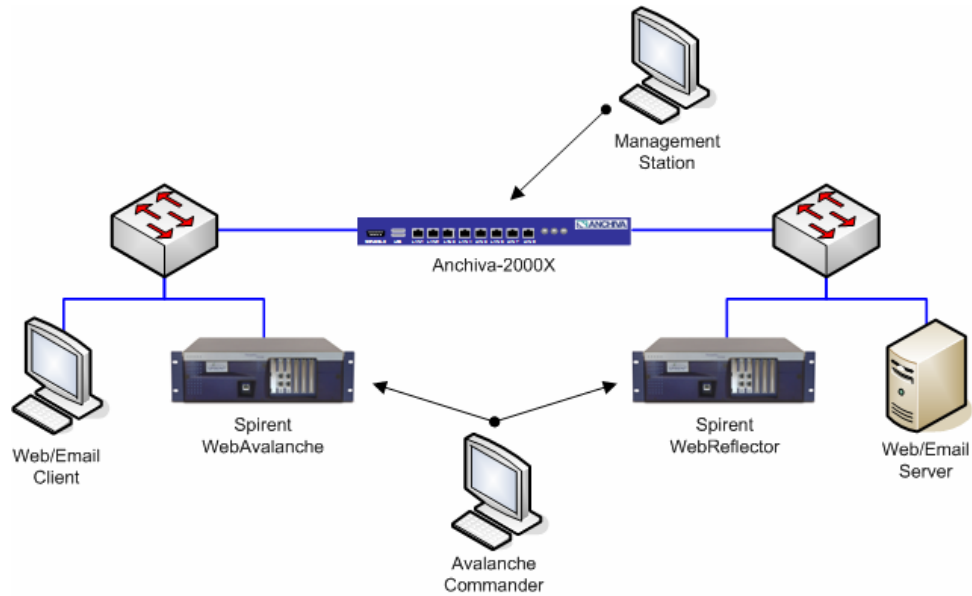
The WebAvalanche was deployed on one side of the Anchiva-2000X to simulate client connections, and the WebReflector was installed on the other side to simulate HTTP and SMTP servers. A client PC was added to the same network as the WebAvalanche, and an HTTP and SMTP server was added to the same network as the WebReflector.

The WebAvalanche and WebReflector were used to generate the traffic and record the results for all of the performance tests, which included throughput test and transaction tests. The standalone client and server were used to attempt to download and send EICAR files through the gateway to verify the Anchiva-2000X could successfully detect and filter malware while under load from the Spirent devices.

Tests were conducted using three different scenarios. The first scenario used HTTP traffic only to simulate deployment of the Anchiva-2000X as an appliance dedicated to protecting a company's internal employees against malicious web sites with malware content. The second scenario was conducted with SMTP traffic only to simulate a deployment protecting a company's email server from virus infected emails. The third scenario was conducted with a mix of both HTTP and SMTP traffic designed to simulate deployment of the Anchiva-2000X as a Web Security Gateway appliance able to protect both LAN and DMZ traffic.

Additional detailed information about each of the tests is included below with the individual test results in the Detailed Findings section of the report.

Test Bed Diagram



Detailed Findings

THROUGHPUT

Section Introduction

ICSA Labs exercised the SUT to determine the maximum throughput that could be achieved in a simulated environment using conditions designed to represent a real-world scenario. These tests were designed to ensure these results could be achieved by the Anchiva-2000X while still maintaining the ability to accurately inspect, forward, and block clean and infected HTTP and/or SMTP traffic.

Findings

Three classes of throughput tests were performed. The first was conducted with HTTP traffic only, the second used SMTP traffic only, and the third scenario used a mix of HTTP and SMTP traffic. These tests were designed to measure the maximum throughput that could be achieved through the Anchiva-2000X with virus scanning enabled.

For these tests, ICSA Labs configured the Spirent WebAvalanche and WebReflector using the following settings:

| Maximum Throughput Test Configuration HTTP Traffic Only | |
|--|--------|
| File Sizes (KB) | 32, 64 |
| Simultaneous Users | 200 |
| Transactions per Sec | 2000 |

| Maximum Throughput Test Configuration SMTP Traffic Only | |
|--|-----|
| Message Size (KB) | 1 |
| Attachment Size (KB) | 30 |
| Simultaneous Users | 100 |
| Transactions per Sec | 100 |

For the traffic mix tests, ICSA Labs configured the Spirent WebAvalanche and WebReflector using the same settings from the HTTP only and SMTP only tests. The HTTP traffic represented 80% of the total traffic load, and the SMTP traffic represented the remaining 20% of the traffic load.

All tests were run three times for a length of 7 minutes. The results from both the first and last minutes of each test were discarded to account for ramp up and ramp down time. The results from the three tests were then averaged for the final results.

ICSA Labs determined the maximum throughput capacity of the Anchiva-2000X when scanning HTTP traffic only was approximately 792 Mbps. When scanning SMTP traffic, the maximum throughput observed was approximately 415 Mbps. A mix of HTTP and SMTP traffic resulted in a maximum of approximately 643 Mbps throughput. The maximum number of packets per second in these tests ranged from over 109,000 for the HTTP only tests to over 92,000 for the SMTP only tests.

| Maximum Throughput Results All Tests | | | | | | |
|---|--------------------------|----------|---------------|--------------------------|-----------|-------------------|
| Traffic Type | Throughput (Mbps) | | | Packet Rate (pps) | | |
| | Inbound | Outbound | Combined | Inbound | Outbound | Combined |
| HTTP | 772.52 | 19.71 | 792.23 | 73,196.64 | 36,166.04 | 109,362.68 |
| SMTP | 26.45 | 388.88 | 415.33 | 50,024.81 | 42,247.36 | 92,272.17 |
| Mix | 463.53 | 179.65 | 643.18 | 64,483.23 | 39,528.39 | 104,011.62 |

TRANSACTIONS

Section Introduction

ICSA Labs exercised the SUT to determine the maximum number of transactions per second that could be achieved in a simulated environment using conditions designed to represent a real-world scenario. These tests were designed to ensure these results could be achieved by the Anchiva-2000X while still maintaining the ability to accurately inspect, forward, and block clean and infected HTTP and/or SMTP traffic.

Findings

Two classes of transaction tests were performed, one with HTTP traffic only and another with SMTP traffic only. These tests were designed to measure the maximum number of transactions per second that could be processed by the Anchiva-2000X with virus scanning enabled.

For these tests, ICSA Labs configured the Spirent WebAvalanche and WebReflector using the following settings:

| Transaction Rate Test Configuration HTTP Traffic Only | |
|--|-----|
| File Size (KB) | 1 |
| Simultaneous Users | 400 |

| Message Rate Test Configuration SMTP Traffic Only | |
|--|-----|
| Message Size (KB) | 1 |
| Attachment Size (KB) | 30 |
| Simultaneous Users | 100 |

ICSA Labs determined the maximum number of transactions per second that could be processed by the Anchiva-2000X when scanning HTTP traffic only was approximately 10,000. When scanning SMTP traffic, the maximum transaction rate was approximately 2,700.

| Maximum Transactions Results All Tests | | |
|---|-----------------------|------------|
| Traffic Type | Number of Connections | |
| | Concurrent | Per Second |
| HTTP | 364.17 | 10,052.19 |
| SMTP | 95.41 | 2,779.93 |

Miscellaneous Notes

Section Introduction

Observations, general notes, and/or specific comments collected during testing by the Premier Services team that did not fall neatly into one of the preceding sections are included below. Note that all observations and comments that follow may be subjective and may have had no bearing on the other testing results.

Comments

The WebUI was very basic and easy to configure. Setup was straightforward and did not require any configuration changes to the pre-existing network infrastructure.

Anchiva's Anchiva-1000 system is currently ICSA Labs certified as an anti-virus gateway. The inspection engine that operates on the Anchiva-1000 is the same engine and signature database that also operates on the Anchiva-2000X.

Conclusion

Anchiva Systems, Inc.'s Anchiva-2000X running AnchivaOS and firmware version 2.0 was able to achieve near gigabit performance in some performance tests. Specifically, the Anchiva-2000X was able to scan over 790 Mbps of HTTP traffic at over 109,000 packets per second. The Anchiva-2000X was also able to process over 10,000 HTTP transactions per second in another test.

Other performance tests revealed that the Anchiva-2000X had the ability to scan over 415 Mbps of SMTP traffic, and could handle over 2,700 SMTP transactions per second. When testing a mix of HTTP and SMTP traffic, the Anchiva-2000X was able to effectively scan over 640 Mbps of traffic.

In all test cases, the Anchiva-2000X was able to successfully detect and block files containing virus content while the system was under load.

Report Summary

Original Report Publication Date

April 18, 2007

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
USA
<http://www.icsalabs.com>

Vendor Headquarters

Anchiva Systems, Inc.
3255 Scott Blvd.
Suite 4-105
Santa Clara, CA 95054-3019
USA
<http://www.anchiva.com>

Copyright

Copyright © 2007 Cybertrust, Inc. All Rights Reserved. No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express permission in writing from ICSA Labs. ICSA Labs is a division of Cybertrust, Inc and is a registered mark of Cybertrust, Inc.